Europ. J. Combinatorics (1990) **11**, 249–266

Some Optimal Codes from Algebraic Geometry and Their Covering Radii†

HEERALAL JANWA

We show that many Goppa codes from algebraic geometry are optimal. Many of these codes attain the Griesmer bound and provide first examples of Griesmer codes which have relatively large dimension compared with the minimum distance. We give a lower bound on the covering radius of algebraic geometric codes in terms of the number of rational points and the genus of the underlying curve. We use this lower bound and some upper bounds on the covering radius proved elsewhere to determine the covering radii of many optimal codes mentioned above exactly. We use our results to give for the first time many non-trivial examples of non-binary normal codes. We also point out connections between our results and many geometric structures such as *saturation configurations, t-independent sets, min-hyper* (*max-hyper*) etc. Finally, we show that Goppa codes have at least the potential of being among the best covering and packing codes discovered so far.

1. INTRODUCTION

A few years ago, V. D. Goppa gave a construction of a class of codes from algebraic curves and related the three fundamental parameters—length, distance and dimension—to the genus and the number of rational points of the curve using the celebrated Riemann–Roch theorem. The main aim of this paper is to try to relate the fourth important parameter of a Goppa code, namely its covering radius to the standard parameters of the curve. In particular, we derive a lower bound on its covering radius which resembles the lower bound on the minimum distance (Section 7). We combine this lower bound with some recent upper bounds on the covering radius (listed in Section 8) to determine the exact covering radii of a class of Goppa codes of small genera (Section 9). The only other classes of q-ary ($q > 2$) codes for which the exact covering radius was known before this are the classical Reed–Solomon codes and the one- and two-error-correcting BCH codes [6]. Before determining the covering radii of the particular Goppa codes, we first show that they are optimal in that they have the smallest length for their dimension and minimum distance. In fact, another major aim of this paper is to show that many Goppa codes are optimal and that many of these meet the Griesmer bound (Section 6). We point out that, even though a search by many people for MDS codes from elliptic curves has been rather fruitless (only one such MDS code has been constructed), there are plenty of other optimal Goppa codes. The third aim is to point out connections between the covering radius problem and the optimality problem and a host of other combinatorial and finite geometric problems (such as min-hyper, max-hyper and saturated configurations). Thus it is hoped to arouse more interest in the problems discussed here.

A brief outline of the paper is as follows. In Sections 2–5 the notations used from algebraic geometry and coding theory are defined and the necessary background from these subjects is discussed. These sections consist of previously known results. As described above, the main original results of this paper are contained in Sections 6, 7

† Presented at the Institute for Mathematics and Its Applications (University of Minnesota) Workshops on Coding Theory and Design theory, June 13–24, 1988.

0195-6698/90/030249 + 18 $02.00/0

and 9. We apply these results to find the first non-trivial examples of non-binary normal codes (Section 10). In Section 11 we connect our work on the covering radius of Goppa codes with some recent results of Brualdi, Pless and Wilson [2]. In Section 12 we establish the connection between the covering radius problem for linear codes and saturated configurations in finite geometry. The existence of Goppa codes is used in Section 13 to derive a lower bound on the maximum length of a linear code with given redundancy and minimum distance.

In order to distinguish new results from those previously published (in Sections 6–7 and 9–13) we quote the latter under the heading 'Proposition'.

2. Background from Algebraic Geometry

For an introduction to algebraic geometry we refer to Chevalley [5] and Hartshorne [15]. We follow Chevalley. For background information on algebraic geometric Goppa codes we refer to the survey article [32]. Also, references [10], [11], [19], [27], [33] and [40] contain an introduction to the necessary concepts from algebraic geometry.

Let F be a *field of algebraic functions* of one variable over the *field of constants* F_q (or simply a *function field of dimension* 1 *over* F_q) in the sense of Chevalley [5].

We follow standard terminology. A list of notation used is as follows:

$PG(r, q)$	the finite projective space of dimension r over F_q
Ω	the module of differentials of F over F_q
(f)	the principal divisor associated with a non-zero element $f \in F$
$\mathrm{Div}(F)$	the divisor group of F written additively
$\deg(D)$	the degree of a divisor D
(ω)	the divisor associated with a differential $\omega \in \Omega$
$\mathcal{L}(D)$	$:= \{f \in F \mid (f) \geqslant -D\}$
$\Omega(D)$	$:= \{\omega \in \Omega \mid (\omega) \geqslant D\}$
g	the genus of F
P	a place of F over F_q
v_P	the valuation of F corresponding to P
$f(P)$	the value of $f \in F$ at P
$res_P(\omega)$	the residue of $\omega \in \Omega$ at P
$\mathrm{sup}(G)$	the support of G, i.e. the set $\{Q_1, \ldots, Q_r\}$, if $g = \sum_{i=1}^{r} a_i Q_i$ and $a_i \neq 0$

We use the *Riemann–Roch* theorem only indirectly in determining the parameters of the algebraic geometric Goppa codes defined in Section 4.

3. Background from Coding Theory

An $[n, k, d]$ q-ary code is a linear subspace of F_q^n of dimension k and minimum Hamming distance d [35].

The *covering radius* of a q-ary block code C of length n is defined as the smallest integer $R = R(C)$ such that all vectors in F_q^n are within Hamming distance R of some codeword of C. For a survey of present knowledge about R, see [6] or [31]. By an $[n, k, d]R$ code we mean an $[n, k, d]$ code having covering radius R. (*Unless otherwise specified, a code in the rest of the paper will mean a linear code.*)

We will need the following facts about R (for references to Facts 3.1–3.5, see [6]).

Fact 3.1. If H is any check matrix of C, then $R(C)$ is the least integer such that every syndrome is an F_q-linear combination of $R(C)$ or fewer columns of H, where a syndrome is any column of length $n - k$ over F_q.

FACT 3.2 (the redundancy bound). $R(C) \leq n - k$.

FACT 3.3 (sphere-covering bound). $q^{n-k} \leq \sum_{i=0}^{R(C)} \binom{n}{i}(q-1)^i$.

FACT 3.4 (Delsarte bound). If s' is the total number of non-zero weights in $C^\perp$, then $R(C) \leq s'$.

FACT 3.5 (The supercode lemma). If C_1 is a proper subcode of C_2, then

$$R(C_1) \geq \max\{\min\{\omega t(x); x \in C_2 \backslash C_1\}, R(C_2)\}.$$

FACT 3.6 [23]. An $[n, 1, n]$ q-ary code has covering radius $\lfloor (q-1)n/q \rfloor$.

A code is called *maximal* if it has no proper supercode with the same length and minimum distance. The following result is proved for $q = 2$ in [6].

FACT 3.7 [23]. A q-ary code C is maximal iff $R(C) \leq d - 1$.

4. ALGEBRAIC GEOMETRIC CODES

Let $P_1, P_2, \ldots, P_n$ be a subset of places of F of degree 1 over F_q. Let $D = P_1 + P_2 + \cdots + P_n$. Let $G \in \mathrm{Div}(F)$ be such that $v_{P_i}(G) = 0$ $(i = 1, \ldots, n)$. (As pointed out by Stichtenoth [40], it is not necessary that G be effective.) Note that such a divisor exists for any degree m, provided that there exists a place P_0 of degree 1 not in $\sup(D)$ (just take $G = mP_0$, $m \geq 0$).

Let $2g - 2 < \deg(G) < n$. Then the F_q-linear map $\phi: \Omega(G - D) \to F_q^n$ given by $\omega \to \phi(\omega) = (\mathrm{res}_{P_1}(\omega), \ldots, \mathrm{res}_{P_n}(\omega))$ is injective by the Riemann–Roch theorem [11].

DEFINITION 4.1. The algebraico-geometric Goppa code is defined as

$$\Gamma(D, G) := \phi(\Omega(G - D)).$$

The next result can be proved using the Riemann–Roch theorem [11].

PROPOSITION 4.1. *$\Gamma(D, G)$ is an $[n, k = n - \deg(G) + g - 1, d \geq \deg(G) - 2g + 2]$ code over F_q.*

The existence of the Goppa codes implied by the following corollary will be used repeatedly in the rest of the paper.

COROLLARY 4.1. *Let D be as above and let $P_0 \notin \sup(D)$ be a place of degree 1 of F. Also let m be an integer such that $2g - 2 < m < n$. Then $\Gamma(D, mP_0)$ is an $[n, k = n - m + g - 1, d \geq m - 2g + 2]$ code over F_q.*

Let $\mathrm{RS}(G, D) := \Gamma(G, D)^\perp$. Then $\mathrm{RS}(D, G) = \psi(\mathcal{L}(G))$, where $\psi: \mathcal{L}(G) \to F_q^n$ is defined by $f \leftarrow (f(P_1), f(P_2), \ldots, f(P_n))$ [34]. The parameters of $\mathrm{RS}(D, G)$ can also be computed using the Riemann–Roch theorem as follows [34].

PROPOSITION 4.2. *Let D and G be as in Proposition* 4.1. *Then $\mathrm{RS}(D, G)$ is an $[n, k = \det(G) - g + 1, d \geq n - \deg(G)]$ code.*

REMARK 4.1. (1) As pointed out in [33], an $\mathrm{RS}(D, G)$ code can still be defined even if D and G do not have disjoint support.

(2) If the upper bound on $\deg(G)$ in Proposition 4.1 is relaxed to $2g-2<\deg(G)<n+2g-2$, then lower bounds on k and d can still be given using the Weierstrass gaps of the points in $\sup(G)$ [10].

5. The Number of Rational Points on Curves over F_q

To construct the best possible Goppa codes from algebraic geometry, we need to find function fields (non-singular absolutely irreducible projective curves) over F_q which have the maximum possible number of places of degree 1 (rational points over F_q) for a given genus g. This maximum number is usually denoted by $N_q(g)$. For applications in Sections 6, 7 and 9, we summarize below the present knowledge about $N_q(g)$.

References to different parts of the following proposition can be found in [19] or [20]. Let $m=\lfloor 2\sqrt{q}\rfloor$.

Proposition 5.1. (1) $N_q(g)\leq q+1+2g\sqrt{q}$ (*A. Weil*);
(2) $N_q(g)\leq q+1+g\lfloor 2\sqrt{q}\rfloor$ (*Serre*);
(3) $N_q(g)\leq q+1-\frac{1}{2}g+\sqrt{(2q+\frac{1}{8})g^2+(q^2-q)g}$ (*Ihara*);
(4) $N_q(g)=q+1+2g\sqrt{q}$ *for* q *square and* $g=\frac{1}{2}(q-\sqrt{q})$ (*Segre*).

Remark 5.1. (1) Some improved results on $N_q(g)$ appear in [41].
(2) For $g>\frac{1}{2}(q-\sqrt{q})$, Proposition 5.1(3) gives a better result than Proposition 5.1(2) (see [19] and [21]).
(3) The Hermitian curve $C: X^{r+1}+Y^{r+1}+Z^{r+1}$ over F_{r^2} contains $N_q(g)=r^3+1$ points (here $q=r^2$) for $g=\frac{1}{2}(q-\sqrt{q})$ [19].
(4) The Deligne–Lusztig curve associated with the Suzuki group (respectively, the Ree group) over F_q, where q is an odd power of 2 (respectively 3), has genus $(q^{\frac{3}{2}}-q^{\frac{1}{2}})/\sqrt{2}$ (respectively, $(\sqrt{3}/2)(q^{\frac{3}{2}}-q^{\frac{1}{2}})+\frac{1}{2}(q^2-q)$) and has q^2+1 (respectively q^3+1) rational points over F_q, which is the maximum permissible for this genus [39].

For genus 1 curves (called *elliptic curves*) much more is known. For the following result and its corollary, see [20] or [38] and the references given there.

Proposition 5.2. *For every integer* $\nu_1=q+1-t$, *with* $|t|\leq m$, *there exists an elliptic curve in* $PG(2,q)$ *having* ν_1 *rational points over* F_q, *provided that* t (*depending upon* q) *is not one of a certain few exceptional values defined in* [38].

Corollary 5.1. *If* $q=p^h$, *then* $N_q(1)=q+m$, *if* p *divides* m, *and* h *is an odd integer* ≥ 3; *otherwise* $N_q(1)=q+1+m$.

Remark 5.2. (1) In some cases (e.g. q is a prime), there are no exceptional values (see [20] and the references therein).
(2) The number of F_q-isomorphism classes of elliptic curves is known: for q a prime, it is $=2q+6$, $2q+2$, $2q+4$, $2q$, for $q\equiv 1, 5, 7, 11 \bmod 12$, respectively (see [29] and the references therein); for general q, we refer to [37].
(3) For some recent computational methods concerning the number of rational points on elliptic curves over F_q, we refer to [26] and [28].

For curves of genus 2, we know the following result of Serre [38].

Proposition 5.3. (1) *If* q *is a square, then* $N_q(2)=q+1+2m$; *except if* $q=4$ *respectively* 9, *then* $N_2(q)=10$ *respectively* 20.
(2) *If* q *is not a square (say,* $q=p^{2e+1}$, p *a prime and* $e\geq 0$), *then define* q *to be special*

if either $p \mid m$ *or* q *is representable by one of the following quadratic polynomials:* x^2+1, x^2+x+1, *or* x^2+x+2 $(x \in \mathbb{Z})$. *Then* $N_q(2) = q+1+m-\delta$, *where* δ *is* 0, 1 *or* 2. (*i*) *If* q *is not special, then* $\delta = 0$. (*ii*) *If* q *is special, then* $\delta = 1$ *or* 2 *depending upon whether* $\{2\sqrt{q} - m\} > (\sqrt{5}-1)/2$ *or not, where* $\{x\}$ *denotes the fractional part of* x.

REMARK 5.3. (1) For more on when q is special, we refer to [38] or [39].
(2) For some conjectures concerning $N_q(g)$, see [38] or [39]. (Seere conjectures that $|N_q(g) - (q+1) - gm| \leq C(g)$, where $C(g)$ depends only on g. Note that, for $g = 1$ or 2, $|N_q(g) - (q+1) - gm| \leq 3$.)
(3) For a table of values of $N_q(1)$ and $N_q(2)$ for $q \leq 128$ and $N_q(3)$ for $q \leq 19$, we refer to [39].
(4) For the best upper bounds on $N_2(g)$, $g \leq 50$, see [38] and [39].
(5) $N_q(4) = 8$, 12, 15 and 18, for $q = 3$, 4, 5 and 25 respectively [39].

6. Optimal Codes from Algebraic Geometry

Let $n_q(k, d) := \min\{n;$ there is an $[n, k, d]$ q-ary code$\}$. The $[n_q(k, d), k, d]$ codes are called *optimal codes*. Much is known about $n_2(k, d)$ and we refer to [43] for a survey. For an arbitrary q, much less is known about $n_q(k, d)$ (see [8] and [12] for the latest results. In a series of papers (e.g. [13] and [14]) Hamada *et al.* have constructed optimal codes over F_q $(q > 2)$ using finite geometric structures known as 'min-hypers'. However, their optimal codes have small k compared with d (i.e. d is near q^k). In this section we use the existence of algebraic geometric codes $\Gamma(G, D)$ with appropriate parameters to determine the exact values of some $N_q(k, d)$ for $q < 2$ and k large.

First, we list some known lower bounds on $N_q(k, d)$. The following result is known as the *Griesmer bound* (see [8] or [14]).

PROPOSITION 6.1. $n_q(k, d) \geq g_q(k, d) := \sum_{i=0}^{k-1} \lceil d/q^i \rceil$.

In some cases the Greismer bound can be improved as follows [8].

PROPOSITION 6.2. *Let* $k \geq q \geq 3$. *Then for any* q *and* d *such that* $2q^i < d \leq q^{i+1}$ *for some* $i \in \{0, \ldots, k-q\}$,

$$n_q(k, d) > g(k, d).$$

Under certain conditions on d and q, it can be shown that $n_q(k, d) = g_q(k, d)$ (see [8] and [12] for further references. Any $[g_q(k, d), k, d]$ code is optimal. Obviously,

$$n_q(k, d) \geq g_q(k, d) \geq k + d - 1.$$

The inequality $n_q(k, d) \geq k + d - 1$ is known as the *Singleton bound.* If $d > q$, then the Singleton bound is always worse than the Greismer bound. $[n, k, d]$ codes with $n = k + d - 1$ codes are called *maximum distance separable* (MDS) codes. The MDS codes are obviously optimal. (See Sections 6.1 and 6.2 for MDS Goppa codes.)

To prove some of the results below, we would also need the following result about $n_q(k, d)$ [8].

PROPOSITION 6.3. *Let* $d = qd_1$. *If* $n_q(k, d) = g_q(k, d)$, *then* $n_q(k, d-a) = g_q(k, d-a)$ *for all* $1 \leq a \leq q-1$. *Conversely, if* $n_q(k, d-a) > g_q(k, d-a)$ *for some* $1 \leq a \leq q-1$, *then* $n_q(k, d-b) > g_q(k, d-b)$ *for all* $0 \leq b \leq a$.

We now show that many $\Gamma(D, G)$ codes are optimal. We refer to Section 14 for optimal RS(D, G) codes.

6.1. *Genus zero.* Proposition 4.1 immediately implies that (as observed by Goppa himelf) these $\Gamma(D, G)$ codes are MDS (hence optimal).

6.2. *Genus one.* They are $[n, k = n - \deg(D), d \geq \deg(D)]$ codes. They correspond to the *elliptic curves*. Obviously, for these codes $k + d \geq n \geq g_q(k, d) \geq k + d - 1$.

If $n = g_q(k, d)$, then we obtain optimal codes, which are MDS if $n = g_q(k, d) = d + k - 1$. For $d \geq q + 1$, we have $g(k, d) \geq k + d$. Thus we conclude the following result.

THEOREM 6.1. *The code* $\Gamma(D, G)$ *with* $\deg(G) \geq q + 1$ *has* $d = \deg(G)$, *and* $n = n_q(n - d, d) = g_q(n - d, d)$.

Therefore, Theorem 6.1 and Corollary 4.1, in conjunction with Proposition 6.2, yield the following.

THEOREM 6.2. *For every* q, *if* $q + 1 \leq d < n < N_q(1)$, *then* $n_q(n - d, d) = g(n - d, d) = n$, *where* $N_q(1)$ *is given by Corollary* 5.1.

Also, $[N_q(1), N_q(1) - d, d]$ optimal codes exist if there is a rational divisor G of degree d composed of places of degree >1.

According to Proposition 5.2 and Remark 5.2, many different (perhaps non-equivalent) elliptic optimal codes guaranteed by Theorem 6.2 exist because many elliptic curves with $n > q + 1$ points exist for most n. In fact, there are many such codes associated with a given elliptic curve. One finds many such codes by taking any subset of its rational points of cardinality greater than $q + 2$ (i.e. many divisors D exist) and by taking any of the several possible divisors G of given degree $\geq q + 1$.

MDS codes when $d \leq q$. MDS codes can be constructed from elliptic curves. For example, [6, 3, 4] MDS codes from the Hermitian curve $X^3 + Y^3 + Z^3 = 0$ over F_4 have been constructed [30], and also by Pellikan [33]. Note that an MDS Goppa code of length 6 over F_4 cannot be constructed from a curve of genus 0, because the maximum possible length is only 5. Exact conditions under which elliptic codes are MDS have been given by Driencourt and Michon using the group law on elliptic curves [10].

The following research problem is from [35, p. 328]:

Given k *and* q, *find the largest value of* n (*denoted* $m(k, q)$) *for which an* $[n, k, n + k + 1]$ *MDS code exists over* F_q.

The determination of $m(k, q)$ is connected with a host of problems in combinatorics and finite geometry (see [16] and [35], Ch. 11). The most interesting unsolved conjecture about $m(q, k)$ is (see [16] for the latest results):

$$m(k, q) = q + 1 \quad \text{for} \quad 2 \leq k \leq q, \quad \text{except for}$$
$$m(3, q) = m(q - 1, q) = q + 2 \quad \text{if} \quad q = 2^k. \quad (6.1)$$

The following is known about elliptic MDS codes. For $q < 13$, there are no MDS codes with lengths greater than the length of previously known codes [25]. For $q \geq 13$, there are no non-trivial elliptic codes of length $n > q + 1$ [25] (see also [10]). It would still be interesting to know which elliptic codes of smaller lengths are MDS (especially the ones with $n = q + 1$). One application of the negative result is that it supports (6.1). As another application, since the elliptic codes have $d = n - k$ or $n - k + 1$, we also conclude the following result.

THEOREM 6.3. *If $q+1<n<N_q(1)$, then the elliptic Goppa codes are optimal.*

Non-MDS optimal codes when $d \leq q$. Even if the condition in Theorem 6.3 is not satisfied, we can still obtain optimal codes from elliptic curves. For example, Dudunekov [8] has shown that for q odd, $n_q(3, q) = g_q(3, q) + 1$. Thus $[q+3, 3, q]$ elliptic codes (there are plenty of such codes) are optimal (as mentioned above, there are no $[q+2, 3, q]$ elliptic MDS codes).

In fact, we can show more. By Proposition 6.2, $n_q(k, d) > g_q(k, d) > g_q(k, d)$ for $2 < d \leq q \leq k$. Therefore, we can conclude the following result.

THEOREM 6.4. *For a given q, if $n < N_q(1)$ and $2 < \deg(G) \leq \min\{q, n-q\}$, then $\Gamma(D, G)$ is an $[n, n-\deg(G), \deg(G)]$ optimal code and $n = n_q(n - \deg(G), \deg(G)) = g_q(n - \deg(G), \deg(G)) + 1$.*

Theorem 6.4 and Corollary 4.1 immediately yield the following result.

COROLLARY 6.1. *For a given q, if $n < N_q(1)$ and $2 < d \leq \min\{q, n-q\}$, then $n_q(n-d, d) = g_q(n-d, d) + 1$.*

Genus two or three. For $g = 2$, the optimality of $\Gamma(D, G)$ depends upon whether $d > \deg(G) - 2g + 2 = \deg(G) - 2$ and upon the behavior of $n_q(k, d)$. For example, we prove the following result.

THEOREM 6.5. *Let m be an integer such that $2 < m < n < N_q(2)$. Let $\Gamma(D, G)$ be an $[n, k, d \geq \deg(G) - 2]$ code from a function field of genus 2, where G is a divisor of degree m (such a G always exists, e.g. G as in Corollary 4.1). Then:*
(1) If $m > q+2$ and $n_q(k, m-2) > g_q(k, m-2) = k+m-2$, then $n_q(k, m-2) = g_q(k, m-2) + 1 = k+m-1$, and $\Gamma(D, G)$ is an $[g_q(k, m-2)+1, k, m-2]$ optimal code.
(2) If $d > m-2 \geq q$, then $n_q(k, m-1) = g_q(k, m-1) = k+m-1$, and $\Gamma(D, G)$ is an $[g_q(k, m-1), k, d = m-1]$ optimal code.
(3) If $d > m-2$ and $n_q(k, m-1) > g_q(m-1)$, then $n_q(k, m-1) = g_q(k, m-1) + 1 = k+m$, and $\Gamma(D, G)$ is an $[g_q(k, m-1)+1, k, d = m-1]$ optimal code.
(4) If $d > m-1$, then $\Gamma(D, G)$ is an $[n, n-m+1, m]$ MDS code.

PROOF. (1) By Proposition 4.1, $\Gamma(D, G)$ is an $[n, k, d \geq m-2]$ code. Since $m-2 > q$, we note that $g_q(k, m-2) \geq k+m-2$. Therefore,

$$n \geq n_q(k, d) \geq n_q(k, m-2) > g_q(k, m-2) = k+m-2 = n-1.$$

Consequently, $n = k+m-1 = n_q(k, d) = g_q(k, m-2)+1$. Since $d \geq m-2 > q$, the Griesmer bound implies that $m-1 = k+n \geq d \geq m-2 > q$. The assumption $m \leq N_q(2)-2$ combined with Proposition 5.3 implies that $2q \geq N_q(2)-3 \geq m-1 \geq d$. Therefore, since $n_q(k, m-2) > g(k, m-2)$, Proposition 6.3 implies that $k+m-1 = n_q(k, d) > g_q(k, d) = k+d \geq k+m-2$. Therefore, $d = m-2$ and $n = n_q(k, d) = g_q(k, d)+1$.

(2) Since $d > q$, the Griesmer bound implies that $n \geq n_q(k, d) \geq g_q(k, d) = k+d \geq (n-m+1)+(m-1)$. Therefore $n = n_q(k, d) = g_q(k, d)$ and $d = m-1$.

(3) and (4) can be proved similarly. □

Note that because of Proposition 5.3, $N_q(2) \gg q+2$ for every $q > 3$. Therefore Theorem 6.5 implies the existence of many good codes. Also, Theorem 6.5(4) demonstrates the possible existence of MDS codes from function fields of genus 2.

A result similar to Theorem 6.5 is also valid for codes of genus 3 with minor modifications. For example, Theorem 6.5(1) is replaced by:

THEOREM 6.6. *Let* $2q+4<m<n<N_q(3)$. *Then* $n_q(k, m-4)>g_q(k, m-4)=m+k-3$ *implies that* $n_q(k, m-4)=g_q(k, m-4)+1=k+m-2$, *and any* $\Gamma(D, G)$ *with* $g=3$ *and* $\deg(G)=m$ *is an* $[n, k-m+2, m-4]$ *optimal code.*

Note that for every q for which we know the values of $N_q(3)$ (Section 4), the condition $2q+4<m<n<N_q(3)$ in Theorem 6.6 is satisfied for some m and n.

Genus greater than three. As examples of good codes from such curves, leg $g=6$ and $q=16$. We know that $N_{16}(6)=65$ (the Hermitian curve C: $X^5+Y^5+Z^5=0$ has 65 points over F_{16}; Proposition 5.1). If $4<m<n<65$, then by Proposition 4.1, we can construct $[n, n-m+5, d\geq m-10]$ codes. If $58<m<n\leq 64$, then the Griesmer bound implies that $n\geq n_{16}(n-m+5, d)\geq n_{16}(n-m+5, m-4)\geq n-3$. Similarly, if $42<m<n-11\leq 53$, then Proposition 4.1 implies that $n\geq n_{16}(n-m+5, m-4)\geq n-3$. Note that the Singleton bound only implies that $n\geq n_{16}(n-m+5, m-4)\geq n-6$.

REMARK 6.1. (1) We can derive additional information about $n_q(k, d)$ from Theorems 6.1–6.5 using Proposition 6.3.
(2) Driencourt and Michon [10] have constructed a $[6, 2, d\geq 4]$ $\Gamma(D, G)$ code with $\deg(G)>\deg(D)$ using the Weierstrass gaps of points in $\sup(G)$ (see also Remark 4.1(2)). We observe that this code meets the Greismer bound. It might be possible to give further examples of optimal codes using their construction.

7. A Lower Bound on the Covering Radius of $\Gamma(D, G)$

In this section we derive lower bounds on $R(\Gamma(D, G))$ which depend upon D and G. For a lower bound on the covering radius of some RS(D, G) codes, we refer to Section 14.

7.1. *Case* I. Let $D=P_1+P_2+\cdots+P_n$ and $G=G_1+G_2+\cdots+G_r$, where $G_j=\sum a_{ij}Q_{ij}$ are the orbits under the Frobenius substitution (i.e. they form the rational decomposition of G over F_q). For example, if $G=mP_0$, then $r=m$ and $G_i=P_0$. We prove the following.

THEOREM 7.1. *Let* D *and* G *be as in Proposition* 4.1. *Then for every* i *such that* $\deg(G)>\deg(G_i)+2g-2$,

$$R(\Gamma(D, G))\geq d(\Gamma(D, G\backslash G_i))$$
$$\geq(\deg(G)-\deg(G_i)-2g+2). \tag{7.1}$$

PROOF. For every i having the stated property, $\Gamma(D, G)$ is a proper subcode of $\Gamma(D, G\backslash G_i)$, of codimension 1 by Proposition 4.1. Therefore, by the supercode lemma (Fact 3.5),

$$R(\Gamma(D, G))\geq d(\Gamma(D, G\backslash G_i))\geq(\deg(G)-\deg(G_i)-2g+2),$$

and the result follows. □

As an immediate application, we have:

COROLLARY 7.1. *Let* $G = G' + P_0$, *where* G' *is rational over* F_q *and* $P_0 \neq P_i$ $(i \in \{1, \ldots, n\})$ *is a place of degree* 1 *such that* $\deg(G) > 2g - 1$. *If we further assume that* D *and* G *are as in Proposition* 4.1, *then*

$$R(\Gamma(D, G)) \geq d(\Gamma(D, G')) \geq \deg(G) - 2g + 1. \tag{7.2}$$

In fact, by using the full strength of the supercode lemma, we can, in some cases, make a stronger assertion than Corollary 7.1. For example, take $G = mP_0$. Then

$$\Gamma(D, G')\backslash\Gamma(D, G) = \{\phi(\omega) \mid (\omega) \in \Omega(G - D);\ \nu_{P_0}(\omega) = (m - 1)\}.$$

Therefore, by the supercode lemma (Fact 3.5), we immediately conclude the following result.

COROLLARY 7.2. *Let* $G = mP_0$, $(m > 0)$ *in Corollary* 7.1. *Then*

$$R(\Gamma(D, G)) \geq \min\{|\phi(\omega)|;\ (\omega) \in \Omega(G - D);\ \nu_{p_0}(\omega) = (m - 1)\}, \tag{7.3}$$

where $|x|$ *denotes the Hamming weight of* x.

Differentials (or functions) having zeros of order precisely $m - 1$ can be studied using *Weierstrass gaps* (see [10] and [41]).

7.2. *Case* II. We assume that there exists a place $P_0 \in \sup(D \cup G)$ which has degree 1. Under the assumption, if $\omega \in \Omega(G - D)$, then $\operatorname{res}_{P_0}(\omega) = 0$.

Therefore,

$$\Gamma(D, G) = \{(c_1, c_2, \ldots, c_n) \mid (0, c_1, c_2, \ldots, c_n) \in \Gamma(P_0 + d, G)\}.$$

In other words, $\Gamma(D, G)$ is a proper shortened subcode of $\Gamma(P_0 + D, G)$ and, by Fact 3.5, we have the following.

THEOREM 7.2. *Let* $P_0 \notin \sup(D \cup G)$ *be a place of degree* 1, *where* D *and* G *are as in Proposition* 4.1. *Then*

$$\begin{aligned} R(\Gamma(D, G)) &\geq \min\{|c| \mid c = (c_0, c_1, \ldots, c_n) \in \Gamma(D + P_0, G);\ c_0 \neq 0\} - 1 \\ &\geq d(\Gamma(P_0 + D, G)) - 1 \geq \deg(G) - 2g + 1. \end{aligned}$$

We obtain the same lower bound as in Corollary 7.1.

8. SOME NEW UPPER BOUNDS ON R

To determine $R(\Gamma(D, G))$ exactly using the lower bounds of the previous section, we need some good upper bounds on R. Some upper bounds on the covering radius of q-ary linear codes are given by Facts 3.1, 3.4 and 3.7. Recently we have proved the following result.

THEOREM 8.1 [22, 23]. *For an* $[n, k, d]$ q*-ary code* C *having covering radius* R,

$$R \leq \mathcal{H}_q(n, k, d) := \mathcal{H}_q(C) := n - \sum_{i=1}^{k} \lceil d/q^i \rceil.$$

In [23] we give the following improvement of the above result.

THEOREM 8.2. *For an $[n, k, d]$ q-ary code C having covering radius $R \leq d$,*

$$R \leq n - n_q(k, d) + d - \lceil d/q^k \rceil \leq \mathcal{H}_q(n, k, d).$$

For such a code a necessary condition for $R = \mathcal{H}_q(n, k, d)$ is that the equality $n_q(k, k) = g_q(k, d)$ hold. Also, a $[g_q(k, d), k, d]$ code can be constructed using C.

Since an $[n_q(k, d), k, d]$ is maximal (by Fact 3.7), Theorem 8.2 yields the following result.

COROLLARY 8.1. *For an $[n_q(k, d), k, d]$ code C, $R(C) \leq d - \lceil d/q^k \rceil$.*

COROLLARY 8.2. *For given k and d, the existence of an $[n_q(k, d), k, d]C$ with covering radius $R = d - \lceil d/q^k \rceil$ implies the existence of an $[n_q(k+1, d), k+1, d]$ code of which C is a shortened code.*

We note that if $n_q(k, d) = g_q(k, d)$, then $n_q(k, d) + \lceil d/q^k \rceil = g_q(k+1, d)$. We can prove the converse to Corollary 8.2 for only the codes meeting the Greismer bound.

COROLLARY 8.3. *For given k and d, any $[g_q(k+1, d), k+1, d]$ code C contains a shortened $[g_q(k, d), k, d]$ subcode with covering radius $R = d - \lceil d/q^k \rceil$.*

REMARK 8.1. Corollaries 8.2 and 8.3 were first proved for binary codes with $n_2(k, d) = g_2(k, d)$ in [4].

Let C be a code (could be non-linear) of length n over F_q. The following upper bounds on R are known as the *Norse bounds* (for $q = 2$, see [6] for the reference; for $q > 2$, see [23]).

THEOREM 8.3. (1) (*i*) *If C has strength* 1, *then* $R(C) \leq \lfloor n(q-1)/q \rfloor$.
(2) (*ii*) *If C has strength* 2 *and is self-complementary, then*

$$R(C) \leq \lfloor (n(q-1) - \sqrt{n})/q \rfloor.$$

For $\Gamma(D, G)$ the strength of the code can be determined from the following result.

PROPOSITION 8.5. *Let $d^\perp$ denote the minimum distance of the dual code of an $[n, k, d]$ code C. Then the maximum strength of C is equal to $d^\perp - 1$. Hence $\Gamma(D, G)$ has strength at least $n - \deg(G) - 1$.*

PROOF. For a proof of the first assertion we refer to [35, pp. 139–140] and the references therein. Since $\mathrm{RS}(D, G) = \Gamma(D, G)^\perp$, the second assertion follows from Proposition 4.2.

9. Exact Covering Radius of Some $\Gamma(D, G)$ Codes

For some comments about the covering radius of $\mathrm{RS}(D, G)$ codes, we refer to Section 14.

Let $\Gamma(D, G)$ be an $[n, k, d \geq \deg(G) - 2g + 2]R$ code from a function field of genus g.

Unless stated otherwise, we will assume throughout this section that D and G are as in Corollary 7.1 *or as in Theorem* 7.2. (9.1)

Then, from (7.1) or (7.2) (as applicable) and Theorem 8.1, we have

$$\mathcal{H}(n, k, \deg(G) - 2g + 2) \geqslant \mathcal{H}(n, k, d) \geqslant R(\Gamma(D, G)) \geqslant \deg(G) - 2g + 1. \quad (9.2)$$

We now prove the following result which determines the exact covering radii of some optimal $\Gamma(D, G)$ codes.

THEOREM 9.1. *Let $\Gamma(D, G)$ be a Goppa code as above such that $n = n_q(k, d)$ and $d = \deg(G) - 2g + 2$. Then $R(\Gamma(D, G)) = \deg(G) - 2g + 1$.*

PROOF. The lower bound comes from (9.2) and the upper bound comes from Theorem 8.2. □

Theorem 9.1 applied to the optimal codes of Section 6 gives us many examples of q-ary codes with known covering radii. In the rest of the section we shed more light on the covering radii of the codes of Section 6.

9.1. *Genus zero.* By Theorem 9.1, these are MDS codes with $R = \deg(G) + 1 = n - k$.

The classical Reed–Solomon (RS) codes are MDS codes, and they are $\Gamma(D, mP_0)$ [11]. For the classical RS codes $R = n - k$ is known [6]. However, not all MDS codes have $R = n - k$. For example, the $[6, 4, 3]$ Hamming code of dimension 3 over F_5 has $R = 1 < n - k$ [6]. We do not know whether this code can be constructed as a $\Gamma(D, G)$ code from a curve of genus 0. As another example, the [6, 3, 4] elliptic MDS code over F_4 mentioned in Section 6.2 has covering radius 2 (see Section 9.2 below). A code of genus 0 is yet to be exhibited which has covering radius unequal to its redundancy.

9.2. *Genus one.* These are $[n, k = n - \deg(G), d = \deg(G)$ or $\deg(G) + 1]$ codes. From (9.2) and Theorem 9.2, we conclude that for the $\Gamma(D, G)$ optimal elliptic codes of Section 6.2, we have $R = \deg(G) - 1$ or $\deg(G)$. Furthermore, by Theorem 9.1, if $d = \deg(G)$ (as in Theorems 6.1–6.4), then $R = \deg(G) - 1$. (Recall that (9.1) is in force.)

If $d = \deg(G) + 1$, then $\Gamma(D, G)$ is an MDS code. First suppose that d and G are as in Corollary 7.1. For this code, if the supercode $\Gamma(D, G\backslash P_0)$ were also MDS, then by Corollary 7.1, we would have $R \geqslant d(\Gamma(D, G\backslash P_0)) > \deg(G) - 1$ implying that $R = \deg(G)$. Similarly, suppose that $\Gamma(D, G)$ is MDS, with D and G as in Theorem 7.2. For this code, if the supercode $\Gamma(D + P_0, G)$ were also MDS, then we would have $R = \deg(G)$.

On the other hand, we can prove the following general result about the covering radius of MDS codes.

LEMMA 9.1. *If C is an $[n, k, n - k + 1]$ MDS code, but there does not exist an $[n + 1, k + 1, n - k + 1]$ MDS code, then $R(C) \leqslant n - k - 1$.*

PROOF. The MDS codes meet the Greismer bound. The result now follows from Corollary 8.3. □

As an application of Lemma 9.1, consider the $[6, 3, 4]$ elliptic MDS code over F_4 mentioned in Section 6.2.1 (which has, by construction, D and G of the type assumed here). By (9.2) it has $R = 2$ or 3. Since there does not exist a $[7, 4, 4]$ MDS code

over f_4 (since $m(4, 4) = 5$ (see [16])), we have $R = 2$. In fact, every $[7, 3, 4]$ MDS code over F_4 has $R = 2$ (because $R > 1$ by the sphere covering bound (Fact 3.3)). Similarly, if conjecture (6.1) is true, then every $[q+1, q-2, 3]$ MDS code over F_q has covering radius 2 provided that $q > 4$. In general, the covering radius of an MDS code of length $m(k, q)$ is strictly less than $m(k, q) - k$.

9.3. *Genus greater than one.* We know the exact covering radii of the optimal codes of Theorems 6.5(1) and 6.6. For some of the other optimal codes the exact covering radii can be determined by using Corollaries 8.1–8.3 and Proposition 6.2, as was done for the elliptic MDS codes above.

10. The Covering Radius of Subcodes and Normal Codes

In a recent survey article on the covering radius of codes [31], it is mentioned that whereas most binary codes seem to be 'normal', it is quite difficult to find non-binary normal codes. In this section we give many non-trivial examples of non-binary normal codes using the results of Section 9. *Throughout this section, C denotes a q-ary $[n, k]R$ code.*

Definition 10.1. Fix $i \in \{1, \ldots, n\}$. For $\alpha \in F_q$, let $C_\alpha^{(i)}$ denote the subcode of C consisting of codewords with ith co-ordinate equal to α. We assume that C is not identically zero at i. Let

$$N^{(i)} := \max\left\{ \sum_{\alpha \in F_q} d(\mathbf{x}, C_\alpha^{(i)}); \mathbf{x} \in F_q^n \right\}. \tag{10.1}$$

Then $N^{(i)}$ is called the norm of C with respect to the co-ordinate position i and $N := \min_{1 \leq i \leq n} N^{(i)}$ is defined to be the norm of C, and co-ordinate positions i for which $N = N^{(i)}$ are called *acceptable.* The code is called *normal* if

$$N \leq qR + (q-1). \tag{10.2}$$

For binary codes, we know the following sufficient condition for normality [7].

Proposition 10.1. *Let C be a binary linear code with covering radius R. If for some i,*

$$R(C_0^{(i)}) \leq R + 2,$$

then C is normal.

This result is false for $q > 2$. For example, let C be the q-ary Hamming perfect code of length $(q^m - 1)/(q-1)$. We show in [24] that $R(C_0^{(i)}) = 3 \leq R(C) + 2$, for $1 \leq i \leq n$. However, C is not normal for $q > 2$, because it has norm $3q - 3$ [31]. We now generalize to all q a slightly weaker version of Proposition 10.1.

Theorem 10.1. *Let C be a q-ary linear code with covering radius R. If for some i,*

$$R(C_0^{(i)}) \leq R + 1,$$

then C is normal.

Proof. Fix an $i \in \{1, \ldots, n\}$. Let $x \in F_q^n$. Since, $C = \bigcup_{\alpha \in F_q} C_\alpha^{(i)}$, there exists a β in F_q such that $d(x, C_\beta^{(i)}) \leq R$. Then.

$$\left\{ d(\mathbf{x}, C_\beta^{(i)}) + \sum_{\alpha \in F_q;\, \alpha \neq \beta} d(\mathbf{x}, C_\alpha^{(i)}) \right\} \leq R + (q-1)(R+1) = qR + (q-1). \tag{10.3}$$

Since the upper bound in (10.3) is independent of $\mathbf{x}$, by (10.1) we have $N^{(i)} \leq qR + (q-1)$. Therefore by (10.2), $N \leq qR + (Q-1)$, implying that C is normal. □

To shed more light on Theorem 10.1, we interpret it as a statement about shortened codes of C. Recall from Section 7, that to obtain the shortened code $SC^{(i)}$ of C at the co-ordinate i,, we just puncture $C_0^{(i)}$ at i. It is immediate that

$$R(SC^{(i)}) = R(C_0^{(i)}) - 1. \tag{10.4}$$

Let H be a check matrix of C. Then a check matrix for $SC^{(i)}$ can be obtained by removing column i of H. Therefore, by the equivalent definition of the covering radius given in Fact 3.1, we obtain the inequality

$$R(C) \leq R(SC^{(i)}). \tag{10.5}$$

Therefore, Theorem 10.1 combined with (10.4) and (10.5) yields the following equivalent sufficient condition for normality of C.

COROLLARY 10.1. *If for some i, $(R(C) = R(SC^{(i)})$, then C is normal.*

To utilize Corollary 10.1, we first need to know more about the covering radius of shortened codes. The following result establishes the equality in Corollary 10.1 for many codes attaining the $\mathcal{K}(n, k, d)$ bound (Theorem 8.1).

THEOREM 10.2. *If $R(C) = \mathcal{K}(C)$ and $d \leq q^k$, then $R(SC^{(i)}) = R(C)$ for all $i \in \{1, \ldots, n\}$.*

PROOF. Fix $i \in \{1, \ldots, n\}$. Since, $SC^{(i)}$ is an $[n, k-1, d_0 \geq d\}$ code,

$$R(SC^{(i)}) \leq \mathcal{K}(n, k-1, d_0) \leq \mathcal{K}(n, k-1, d) = \mathcal{K}(n, k, d) + \lceil d/q^k \rceil. \tag{10.7}$$

The result now follows from the conditions given (i.e. $R(C) = \mathcal{K}(n, k, d)$ and $n \leq d/(q^k)$). □

In Section 9, we gave examples of many Goppa codes C for which $R(C) = \mathcal{K}(C)$ and $d \leq q^k$. Thus we have non-trivial examples of many q-ary normal codes for $q > 2$. By shortening such codes, we obtain more normal codes.

For D and G as in Section 7.2, a lower bound on the covering radius of the shortened $\Gamma(D, G)$ is also provided by Theorem 7.2.

11. SHORT CODES WITH A GIVEN COVERING RADIUS

In this section we connect our work on the covering radius of $\Gamma(D, G)$ with some recent results of R. Brualdi, V. Pless and R. Wilson [2]. In particular, we show that their results provide improved lower bounds on the covering radius of the codes of Section 7. On the other hand, we show that the algebraic geometric codes have the potential of being very good covering codes. In fact, we show that many of these codes may improve some results in the articles cited and therefore require further study.

In [2] the length function $l(m, r; q)$ is defined to be the smallest length of a code over F_q of codimension m and covering radius r. For $q = 2$ the length function has received a lot of attention recently because it efficiently presents all the information about the covering radius function $t[n, k]$, which is defined to be the smallest covering radius of a k-dimensional binary code of length n.

Though only $l(m, r; 2)$ has received much attention, the following result from [2] shows that the knowledge of $l(m, r; q)$ (for $q = w^h$) is very useful for the binary length function.

PROPOSITION 11.1. $l(km, r; q) \leq \dfrac{(q^k - 1)}{(q - 1)} l(m, r; q^k)$.

This gives us a lower bound on $l(m, r; q^k)$ if we know a lower bound on $l(km, r; q)$. A table of good lower bounds on $l(m, r; 2)$ for $m \leq 24$ is given in [1]. We can use these values to derive better lower bounds on some $R(\Gamma(D, G))$ over F_{2^k} (for $m \leq 24$) than the ones given by (7.1)–(7.3). Conversely, we show that if a lower bound in (7.1)–(7.3) is attained for some lengths, then it could lead to improvements on the upper bound on $l(m, r; 2)$ (given in [2] or [1]) for some m and r. We illustrate these applications with a few examples. Let $\Gamma(D, G)$ be any $[n, n - \deg(G) + 1, d \geq \deg(G) - 2]R \geq \deg(G) - 3$ genus 2 Goppa code over F_q with D and G as in Section 7.1 or 7.2. From [1] and [2], we have $l(4, 2; 16) \geq l(16, 2; 2)/15 \geq 25$ and $l(4, 2; 8) \geq 13$. Therefore any $[n \leq 24, n - 4, d \geq 3]R \geq 2$ genus 2 Goppa code over F_{16} described above has R at least 3 (and at most 4 by Fact 3.1), and any $[n \leq 12, n - 4, d \geq 2]R \geq 2$ Goppa code over F_8 of the above type has R at least 3. Similarly, any such $[n \leq 12, n - 5, d \geq 4]R \geq 3$ Goppa code over F_8 has R at least 4. Also, any $[6, 3, d \geq 3]$ elliptic Goppa code over F_{16} has $R = 3$ because $l(3, 2; 16) \geq 7$.

Conversely, if any of the $[20 \geq n \geq 13, n - 5, d \geq 4]R \geq 3$ Goppa code over F_{16} has $R = 3$, then by Proposition 11.1, $l(20, 3; 2) \leq 15l(5, 3; 16) \leq 15n \leq 300$, which is an improvement on the upper bound 308 on $l(20, 3; 2)$ given in [1]. (Note that there exist many codes from curves of genus 2 with $20 \geq n \geq 13$, since, by Proposition 5.1, $N_{16}(2) = 33$.)

12. Saturated Configurations and Covering Radius

We first relate the covering radius problem for linear codes to 'saturated configurations' in finite projective spaces introduced in [42]. We then show that many good configurations of these types can be constructed using some particular type of linear codes (among them the $\Gamma(D, G)$ codes).

DEFINITION 12.1 [42]. Let K be a set of k points in $PG(r, q)$ $(k \geq r + 1)$. Then K is said to be ρ-saturated for some integer ρ $(1 \leq \rho \leq r - 1)$ if, for any point $x \in PG(r, q)$, there exist $\rho + 1$ independent points $x_0, \ldots, x_\rho \in K$ so that x lies in the subspace $\langle x_0, \ldots, x_\rho \rangle \subseteq PG(r, q)$. The set K is called *minimal* ρ-saturated if $K \backslash \{x\}$ is not ρ-saturated for any choice of $x \in K$. Let $k(r, q, \rho) :=$ the smallest k for which there exists a ρ-saturated set of size k in $PG(r, q)$.

We can interpret a ρ-saturated configuration K in $PG(r, q)$ as a linear $[k, k - (r + 1)]$ q-ary code with covering radius $\leq \rho + 1$ as follows. We first identify the points of $PG(r, q)$ with equivalence classes of $(r + 1)$-tuples over F_q. Let C be the code having an $(r + 1) \times k$ check matrix H, the columns of which represent the elements of K as $(r + 1)$-vectors (we obtain equivalent codes by picking different representatives for the projective points). The rank of H is $r + 1$ by the definition of K. Also, Fact 3.1 implies that $R \leq \rho + 1$. To say that K is minimal ρ-saturated is equivalent to saying that $R(SC^{(i)}) > R(C)$ for $1 \leq i \leq k$ (see the proof of (10.5)).

Conversely, given an $[n, k, d]R$ q-ary code C and a check matrix H, the columns of H give us an $(R - 1)$-saturated configuration. It is minimal if the covering radius of

each of its shortened subcodes is strictly larger than R. Note that different H matrices give possibly different saturated sets. For $q=2$ many cyclic codes give minimal saturated configurations (see [9] and [24]).

Note that in the above setting, the integer $k(r, q, \rho)$ equals $l(r+1, \rho+1; q)$ defined in the previous section. (Obviously $k(r, q, \rho) \leq l(r+1, \rho+1; q)$. Conversely, if $k = k(r, q, \rho)$, then there exists a $[k, k-r-1]R \leq \rho+1$ code. Therefore, $k \geq l(r+1, R; q) \geq l(r+1, \rho+1; q)$ from (2.6) in [2].) The article [42] lists some upper and lower bounds on k and $k(r, q, \rho)$ (and hence on $l(r+1, \rho+1; q)$). For the fields of characteristic 2, the upper bounds on $l(r, q, \rho)$ given in [2] are slightly better than the ones given in [42]. For example, $l(3, 1; q) \leq 2q+1$ from the proof of Theorem 3.2 in [2]. However, Lemma 5 in [42] yields $l(3, 1; q) \leq 2q+2$.

From the discussion in the last section, the codes $\Gamma(D, G)$ have the potential of yielding many good saturated configurations. Finally, we note the following simple consequence of the supercode lemma (Fact 3.5).

THEOREM 12.1. *An $[n, k, d]R$ code always yields a minimal $(R-1)$-saturated configuration, provided that $R > d-1$.*

13. THE MLCT PROBLEM

For fixed d and q consider the following two problems [16].

PROBLEM 13.1. For n, find the maximum dimension k such that there exists an $[n, k, d]$ code over F_q. This problem is referred to as the *main linear coding theory problem* (or MLCT problem).

Solving Problem 13.1 for all n (and given q and d) is equivalent to solving the following version of the MLCT problem for all r [16].

PROBLEM 13.2. For given redundancy r, find the maximum length n (denoted $\max_{d-1}(r, q)$) such that there exists an $[n, n-r, d]$ code.

For $d-1=r$ (i.e. for MDS codes), $\max_{d-1}(r, q)$ equals the function $m(r, q)$ defined in Section 6.1. By looking at a parity check matrix of an $[n, n-r, d]$ code with $n = \max_{d-1}(r, q)$, it follows that $\max_{d-1}(r, q)$ is the largest set of vectors in $PG(r-1, q)$ such that any $d-1$ of them are linearly independent. This *packing problem* for $PG(r-1, q)$ has been extensively studied in connection with the design of experiments in statistics by Bose and others (see [20]). For the present knowledge about $\max_{d-1}(r, 3)$, see [17].

We use the existence of $\Gamma(D, G)$ for certain D and G to prove the following lower bound on $\max_{d-1}(r, q)$.

THEOREM 13.1. *For $0 \leq s < N_q(g) - 2g$,*

$$\max_s (s+g, q) \geq N_q(g) - 1.$$

PROOF. There exists a function field of genus g over f_q with $N = N_q(g)$ places of degree 1, say $P_1, \ldots, P_N$. Then, by Corollary 4.1, $\Gamma(D, G)$ with $D = P_1 + \cdots + P_{N-1}$ and $G = mP_N$ is an $[n = N-1, n-m+g-1, d \geq m-(2g-2)]$ code, provided that $2g-2 < m < N-1$. Since $r = n-k = m-g+1$, we have $d-1 \geq r-g$. Therefore, $\max_{d-1}(r, q) \geq N_q(g) - 1$, where $g-1 < r < n-g+1$ and $r-g \leq d-1$. The result now follows because $\max_{r-g}(r, q) \geq \max_{d-1}(r, q) \geq N_g(g) - 1$, for $r-g \leq d-1$. □

The lower bound can be improved by 1, if there is a rational divisor G of degree r. Further improvement depends upon whether the lower bound on d in Theorem 4.1 can be improved.

14. Optimality and Covering Radii of RS(D, G) Codes

Our proof of the optimality of a $\Gamma(D, G)$ code in Section 6 does not depend upon the structure of the divisor G, but only upon $\deg(G)$ and the lower bound $d \geq \deg(G) - 2g + 2$ given by Proposition 4.1. By Propositions 4.1 and 4.2, a $\Gamma(D, G)$ code and an RS(D, G') code with $\deg(G') = n - \deg(G) + 2g - 2$ have the same n and k, and the same lower bound on their respective minimum distance. (Note that $2g - 2 < \deg(G) < n$ iff $2g - 2 < \deg(G') < n$. Therefore G and G' satisfy the conditions of Propositions 4.1 and 4.2 respectively.) Hence, if $\Gamma(d, G)$ can be shown to be optimal by the methods of Section 6, then RS(D, G') is also optimal.

A lower bound on the covering radius of some RS(D, G) codes can be derived in the same fashion we derived the lower bound on the covering radius of particular $\Gamma(D, G)$ in Theorem 7.1. Let D and G be as in Section 7.1. Then Theorem 7.1 is replaced by:

For every i such that $\deg(G) > \deg(G_i) + 2g - 2$,

$$R(\mathrm{RS}(D, G\backslash G_i)) \geq d(\mathrm{RS}(D, G)) \geq (n - \deg(G)).$$

Therefore Corollary 7.1 is replaced by:

Let $G = G' + P_0$, where G' is rational over F_q and P_0 ($\neq P_i$, $i \in \{1, \ldots, n\}$) is a place of degree 1 *such that* $\deg(G) > 2g - 1$. *If we further assume that D and G are as in Proposition* 4.1, *then*

$$R(\mathrm{RS}(D, G\backslash P_0)) \geq d(\Gamma(D, G)) \geq n - \deg(G).$$

We can combine this lower bound with the upper bounds on R given in Section 8 to determine exactly the covering radii of many optimal RS codes.

The weight distributions of some $\Gamma(D, G) = RS(d, G)^{\perp}$ codes have been determined in [25]. Therefore we can use the Delsarte bound (Fact 3.5) to give an upper bound on the covering radius of RS(D, G) codes. It has been shown in [25] that many $\Gamma(D, G)$ codes are self-dual.

Acknowledgements

The author is indebted to Professor H. F. Mattson Jr. and Dr. R. Dougherty for constructive criticism and helpful suggestions. He is also thankful to the referees for some helpful comments in clarifying the manuscript.

References

1. R. Brualdi and V. Pless, On the length of codes with a given covering radius, Preprint.
2. R. Brualdi, V. Pless and R. M. Wilson, Short codes with a given covering radius, *IEEE Trans. Inform. Theory*, **IT-35** (1) (1989), 99–109.
3. A. A. Bruen, J. A. Thas and A. Blokhuis, On MDS codes, arcs in $PG(n, q)$ with q even, and a solution of three fundamental problems of B. Segre, *Invent. Math.*, **92** (1988), 441–459.
4. P. B. Busschbach, M. G. L. Gerretzen and H. C. A. van Tilborg, On the covering radius of binary, linear codes meeting the Griesmer bound, *IEEE Trans. Inform. Theory*, **IT-31** (1985), 465–468.
5. C. Chevalley, *Introduction to the Theory of Functions of One Variable*, A.M.S. Math. Surveys, New York, 1951.

6. G. D. Cohen, M. G. Karpovsky, H. F. Mattson, Jr. and J. R. Schatz, Covering radius—survey and recent results, *IEEE Trans. Inform. Theory,* **IT-31** (1985), 328–343.
7. G. D. Cohen, A. C. Lobstein and N. J. A. Sloane, Further results on the covering radius of codes, *IEEE Trans. Inform. Theory,* **IT-32** (1986), 680–694.
8. S. M. Dodunekov, Minimum block length of a linear q-ary code with specified dimension and code distance, *Prob. Inform. Transmission* **20** (1985), 239–249.
9. R. Dougherty and H. Janwa, Covering radius computations for binary cyclic codes, *Maths Comp.* (submitted).
10. Y. Driencourt and J. F. Michon, *Rapport sur les codes Géométriques,* Université Aix-Marseille II et Université Paris 7, 1986.
11. V. D. Goppa, Codes and information, *Russian Math. Surv.*, **39** (1985), 87–141.
12. N. Hamada and M. Deza, Characterization of $\{2(q+1)+2, 2; t, q\}$-min-hyper in $PG(t, q)$ $(t \geq 3,\ q \geq 5)$ and its applications to error-correcting codes, *Discr. Math.*, **71** (1988), 219–231.
13. N. Hamada and M. Deza, Characterization of $(n, k, d; q)$-codes meeting the Griesmer bound for given integers $k \geq 3,\ q \geq 5$ and $d = q^{k-1} - q^{\alpha} - q^{\beta} - q^{\gamma}$ $(0 \leq \alpha \leq \beta < \gamma < k-1$ or $o \leq \alpha < \beta \leq \gamma < k-1)$, Preprint.
14. N. Hamada and F. Tamari, Constructions of optimal linear codes using flats and spreads in finite projective geometry, *Europ. J. Combin.* **3** (1982), 129–141.
15. R. Hartshorne, *Algebraic Geometry,* Springer-Verlag, New York, 1977.
16. R. HIll, *A first Course in Coding Theory,* Oxford University Press, Oxford, 1986.
17. R. HIll and D. E. Newton, Some optimal ternary linear codes, *Ars Combin.*, **25A** (1988), 61–72.
18. J. W. P. Hirschfeld, *Projective Geometries over Finite Fields,* Clarendon Press, Oxford, 1979.
19. J. W. P. Hirschfeld, Linear codes and algebraic curves, in: *Geometrical Combinatorics* (F. C. Holroyd and R. J. Wilson, Pitman, Boston, 1984, pp. 35–52.
20. J. W. P. Hirschfeld, *Finite Projective Spaces of Three Dimension,* Clarendon Press, Oxford, 1985.
21. Y. Ihara, Some remarks on the number of rational points of algebraic curves over finite fields, *J. Fac. Sci. Univ. Tokyo, Sect. IA, Math.*, **28** (1981), 721–724.
22. H. Janwa, Some new upper bounds on the covering radius of binary linear codes, *IEEE Trans. Inform. Theory,* **IT-35** (1) (1989), 110–122.
23. H. Janwa, On the covering radius of q-ary codes, Presented at the 7th International Conference on Applied Algebra and Error-Correcting Codes (AAECC-7), Toulose, France, June 26–30, 1989.
24. H. Janwa, The covering radius and normality of t-dense codes (in preparation).
25. G. L. Katsman and M. A. Tsfasman, Spectra of algebraic-geometric codes, *Probl. Inform. Transmission,* **23** (1988), 262–275.
26. A. D. Keedwell, Simple constructions for elliptic cubic curves with specified small numbers of points. *Europ. J. Combin.*, **9** (1988), 463–481.
27. G. Lachaud, Les codes geometriques de Goppa, *Séminaire Burbaki* **641** (1985); *Asterisque,* No. 133–134 (1986), 189–207.
28. S. E. Landsburg, p-Adic cohomology and zeta functions of elliptic curves, Queens Papers in Pure Mathematics, 1986.
29. H. W. Lenstra, Factoring integers with elliptic curves, *Ann. Math.*, **126** (1987), 649–673.
30. C. M. Liu and P. Vijay Kumar, On the maximum length of MDS Goppa codes on elliptic curves. Preprint.
31. J. H. van Lint, Recent results on covering problems, Proceedings of the 6th International Conference on Algebraic Algorithms and Error-correcting Codes, Rome, July 1988. Lecture Notes in Computer Science (357).
32. J. H. Van Lint, Algebraic geometric Goppa codes, Preprint of a paper submitted to the Proceedings of the Workshops on Coding Theory and Design theory, Institute for Mathematics and Its Applications (University of Minnesota) June 13–24, 1988.
33. J. H. van Lint and G. van der Geer, *Introduction to Coding theory and Algebraic Geometry,* Birkhäuser Verlag, Basel, 1988. DMV Seminar, Band 12.
34. J. H. van Lint and T. A. Springer Generalized Reed–Solomon codes from algebraic geometry, *IEEE Trans. Inform. Theory,* **IT-33** (1987), 305–309.
35. F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-correcting codes,* North Holland, Amsterdam, 1977.
36. C. J. Moreno, *Algebraic Curves over Finite Fields and Error-Correcting Codes,* Cambridge University Press (to appear).
37. R. Schoof, Nonsingular plane cubic curves over finite fields, *J. Combin. Theory Ser. A,* **46** (1987), 183–211.
38. J.-P. Serre, Nombres de points des courbes Albébriques sur F_q, *Séminaire de Théorie des Nombres de Bordeaux exposé 22 (1982–1983)*, 1–8.

39. J.-P. Serre, Rational points on curves over finite fields q Large: Parts I and II, Lectures given at Harvard University September–December 1985. Notes by Fernando Gouvea.
40. H. Stichtenoth, Self-dual Goppa codes, *J. Pure Appl. Algebra*, **55** (1988), 199–211.
41. K. O. Stöhr and J. F. Voloch, Weierstrass points and curves over finite fields, *Proc. Lond Math. Soc.*, **50** (3) (1986), 1–19.
42. E. Ughi, Saturated configurations of points in projective Galois spaces, *Europ. J. Combin.* **8** (1987), 325–334.
43. T. Verhoeff, An updated table of minimum-distance bounds for binary linear codes, *IEEE Trans. Inform. Theory*, **IT-33** (5) (1987), 665–680.

Received 22 January 1989 and revised version accepted 19 September 1989

HEERALAL JANWA
Department of Mathematics
California Institute of Technology,
Pasadena, California 91125, U.S.A.